THE HONORABLE JOHN C. COUGHENOUR

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE**

ZANGO, INC. , Plaintiff, v. PC TOOLS PTY, LTD., Defendant.	Case No. 07-CV-00797-JCC **DECLARATION OF BENJAMIN G. EDELMAN IN SUPPORT OF DEFENDANT'S OPPOSITION TO MOTION FOR TEMPORARY RESTRAINING ORDER**

1. I, Benjamin G. Edelman, certify and declare as follows:

2. I make this declaration under penalty of perjury and from my own personal knowledge. I am over the age of eighteen years and competent to testify to the matters herein. The opinions set forth below are made to a reasonable degree of professional certainty.

3. I have been retained by defendant PC Tools as an expert in the above-captioned matter.

4. Attached hereto as **Exhibit A** is a true and correct copy of my current Curriculum Vitae.

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

Dockets.Justia.com

Education, Employment History and Related Experience

5. I am an assistant professor at Harvard Business School, where my research focuses on the design of electronic marketplaces, with an emphasis on designing markets to prevent fraud.

6. I hold a Ph.D. from the Harvard Graduate School of Arts and Sciences in Economics, a J.D. from Harvard Law School, an A.M. from the Harvard Graduate School of Arts and Sciences in Statistics, and an A.B. from Harvard College in Economics.

7. I have also taken on a variety of outside consulting projects. To the extent that these projects have culminated in expert testimony, they are detailed in the section that follows, Prior Expert Testimony. Representative examples of my non-litigation consulting projects include tracking large-scale domain name registrations that infringe on the rights of others, assisting web sites blocked by China in reconfiguring their servers to be reachable to users in that country, and detecting fraudulent requests for payment of certain online advertising commissions.

8. Until January 2004, I was employed as a Student Fellow at the Berkman Center for Internet & Society at Harvard Law School. My work at the Berkman Center included original research on all aspects of the Internet's design, operation, and use, with a focus on domain names, filtering, electronic commerce, and multimedia. Between 1998 and 2001, I had operational responsibility for the Berkman Center network, including setting up and maintaining server, network and PC equipment; and designing web content, including database-generated web sites and web interfaces to database data.

9. Between 1996 and 1998, I was employed as a technical consultant at Stand for Children, a non-profit organization in Washington, DC. My responsibilities at Stand for Children included setting up server, network, and PC equipment; providing technical support; designing databases and database user interfaces; and designing web interfaces to database data.

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

Prior Expert Testimony

10. I have been retained as a consulting expert in a number of pending and completed matters, and I have provided oral expert testimony in five matters.

11. In 2000, I was asked by the National Football League to study the security systems and methods of transmission used by iCraveTV, a Canadian company retransmitting American network television content over the Internet. My work for the National Football League investigated the means of determining the geographic location of users receiving certain streaming video content as well as the nature and effectiveness of security systems restricting access to that content. My work culminated in providing oral testimony in the United States District Court for the Western District of Pennsylvania in a lawsuit captioned *National Football League, et al., vs. TVRADIONOW Corporation, et al.*, No. CIV.A. 00-120 and 00-121, 2000 U.S. Dist. LEXIS 1013 (W.D. Pa. 2000).

12. In 2000, I was asked by the American Civil Liberties Union to study the design of certain commercial Internet filtering products. My work for the ACLU investigated the capabilities and limitations of proposed methods of filtering access to certain types of Internet content. In 2002, my work culminated in qualification as an expert in the United States District Court for the Eastern District of Pennsylvania, where I provided oral testimony in a lawsuit captioned *Multnomah County Public Library v. United States of America*, No. Civ.A. 01-1322, 2002 WL 1126046 (E.D. Pa. 2002).

13. In 2001, a group of media companies asked me to study software provided by The Gator Corporation. Gator software showed targeted pop-up ads according to users' web browsing activities. My work for these media companies investigated the methods of advertising display used by Gator as well as its methods of installation and targeting. I served as an expert in the lawsuit captioned *Washingtonpost.Newsweek Interactive Company, LLC, et al. v. The Gator Corporation*, No. Civ.A. 02-909-A (E.D. Va. 2002).

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

14. In 2003, Quicken Loans and Wells Fargo asked me to study software provided by WhenU.com. My work for Quicken Loans and Wells Fargo investigated the design of WhenU software, including the specific method of targeting of particular WhenU advertisements to be shown when users visit particular web sites. I served as an expert and gave oral testimony in a matter captioned *Wells Fargo & Company, et al., v. WhenU.com, Inc.*, which is reported at 293 F. Supp. 2d 734 (E.D. Mich. 2003).

15. In 2004, the State of Utah asked me to study the method of operation of software provided by WhenU. My work included examining the means by which WhenU software identifies its location of installation, as well as methods by which WhenU could keep its software out of the state of Utah. I also studied WhenU's installation methods and the disclosures shown to users in the course of installing WhenU software. I served as an expert and gave oral testimony in the matter captioned *WhenU.com, Inc. v. The State of Utah*, Civ.No. 040907478 (Ut. 2004).

Zango's Software Generally

16. Zango makes software that shows intrusive advertisements on users' computers, typically in the form of pop-up ads. As a user browses the web, Zango tracks what web sites the user visits and what keywords the user searches for. Zango then shows pop-up ads that cover the user's web browser, often filling the user's entire screen and preventing the display of the content the user had actually requested. Only if the user specifically closes such a pop-up can the user return to the task the user had intended. The resulting distraction and delay come at a cost to productivity: The user can't do what he intended as quickly on a computer with Zango as he could on an ordinary computer.

17. Zango's advertising software is not software users affirmatively seek or request. Instead, users must be induced to install Zango software through a ruse. Typically, Zango (or a Zango partner) offers a trinket some users might want, at least if the trinket came with no strings attached. But before users can access that trinket, Zango forces users to agree to receive Zango

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

pop-up ads also. The presence of Zango's pop-up ad software is almost never mentioned at the outset of the offer (i.e. when users first notice the trinket and first begin to evaluate it). Instead, users learn about Zango's advertising only after beginning the process of receiving the trinket. Furthermore, as set out below, Zango's descriptions of its programs are vague at best, and in some cases missing altogether.

The Effect of Zango on Users' Privacy

18. Zango's software demands a substantial compromise of users' privacy. As a user browses the web on a computer with Zango software installed, Zango transmits detailed information to its servers about the specific web sites and web pages the user visits, and about the specific keywords the user searches for. Each such transmission includes a user ID number that uniquely identifies the user's computer. Each such transmission also carries detailed information about the user's computer, including the user's IP address, which in many instances can be linked back to a specific identifiable user.[1]

19. Zango's privacy policy[2] promises to limit the uses of the information Zango collects. For example, Zango promises that it will not use a user's IP address to identify a user personally, unless required by law. But in practice, users have no way to verify that use or non-use. Zango could exploit users' information in a way Zango's privacy policy prohibits, and users would have no way to know.

20. Even if Zango fully complies with its privacy policy, its data may nonetheless become available to third parties in ways that concern typical users. If served with a subpoena, Zango is likely to be able to identify the web browsing of a specific user – including specific sites visited and specific searches conducted.[3] In contrast, for a user without Zango, gathering

---

[1] See e.g. http://cyber.law.harvard.edu/people/edelman/pubs/icrave-012700.pdf, ¶13
[2] http://www.zango.com/destination/corporate/privacypolicy.aspx
[3] Given a user's unique Zango ID number or the user's IP address, Zango could report browsing and searches associated with that user.

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

this information is likely to require a physical intrusion into the user's residence. Users seeking to retain their privacy are therefore unlikely to want Zango software on their computers.

Zango's Historical Activities

21. I have studied Zango software since 2003, and I have observed a wide variety of improper and controversial activities.

Zango's Installation Methods

22. Through 2005 and continuing into early 2006, Zango software was widely installed without consent. Zango paid thousands of third party "distributors" to install its software, without any bona fide investigation of the distributors' methods. For example, Zango accepted as distributors a 21-year-old hacker[4] from Oklahoma[5], a 20-year-old California hacker who attacked Defense Department computers,[6] and unnamed individuals from locations as far-flung as Lebanon and Slovenia.[7] Zango even recruited new distributors via spam.[8]

23. Zango claims it required its distributors to obtain user consent before installing Zango software. But in practice, distributors had little incentive to seek user consent. If users were asked to accept Zango, many would refuse. In contrast, a distributor that simply installed Zango (without requesting users' permission) could get payment for installation on more computers, thereby receiving larger payments from Zango.

24. These practices continued for years until, in early 2006, Zango finally took action. But in the interim, tens of millions of computers became infected with Zango's software, often without users agreeing to install it. These installations came at an untold cost to users, often novices, who then had to figure out what was wrong with their computers and how to fix it.

---

[4] http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342_pf.html
[5] http://fishbowl.pastiche.org/2006/02/19/the_perils_of_metadata
[6] http://www.spamdailynews.com/publish/Alleged_zombie_master_arrested.asp
[7] http://www.vnunet.com/vnunet/news/2141283/adware-makers-sues-naughty
[8] http://www.benedelman.org/spyware/180-affiliates/installation.html#email

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

25. Zango software was also often installed via hidden disclosures. In many instances, users would have had to scroll past multiple pages of irrelevant text in order to learn that Zango pop-up ads would be installed too. For example, a user would be unlikely to learn that installing Kiwi Alpha installs Zango too, because that disclosure begins at page 16 of a 54-page license agreement.[9] If a user simply pressed "Next" without scrolling through the lengthy box, Zango software would become installed onto the user's computer without the user fairly agreeing.

Zango's Unlabeled Advertisements

26. Historically, Zango advertisements have not always carried Zango labeling. Many Zango ads included "redirects" or other computer code that eliminated ad labeling. As a result, Zango showed on-screen pop-up ads without any indication that the ads came from Zango rather than from some other source.

27. The absence of Zango labeling is particularly pernicious when users didn't agree to install Zango in the first place. Such users face extra difficulty in finding the source of unwanted pop-ups and in making those pop-ups stop.

28. Zango claims to have stopped unlabeled pop-ups. But technology research group the Center for Democracy and Technology (CDT) in 2006 observed 39 distinct unlabeled Zango ads.[10] I too have seen unlabeled Zango ads as recently as November 2006.[11]

Zango's Use of Randomized Product Names, Folders, and Filenames

29. Zango software has used a series of different names, including n-Case, 180search Assistant, Zango, and Seekmo. All these programs share a common core function – tracking users' online activities, and showing pop-up ads. Furthermore, these programs also share a common method of communications with Zango servers. Yet these programs have used multiple distinct names. The repeated name changes serve to confuse consumers – preventing consumers

---

[9] http://www.benedelman.org/spyware/180-affiliates/installation.html#license
[10] http://www.ftc.gov/os/comments/zango/zango/index.php
[11] http://www.benedelman.org/news/112006-1.html#h

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

from associating a new Zango product name with the prior bad practices consumers had previously come to distrust.

30. Zango software has also used a wide variety of filenames, including randomly-named and arbitrarily-named files that hinder users' efforts to identify and remove Zango software. For example, Zango programs have used files named 180ax*, 180sa.*, msbb.* saap.*, sain.*, salm.*, and sau.*.

31. Zango has placed its files in a wide variety of locations on users' computers. Zango has placed its files in c:\, c:\Windows, c:\Windows\System, c:\Windows\System32, c:\Temp, and even within various subfolders of c:\Documents and Settings\[username]. These many placements are contrary to Windows standards, which instead call for placement within a single clearly-named subfolder of c:\Program Files. The effect of these arbitrary placements is to further hinder users' efforts to identify and remove Zango software.

Response to Zango's Historical Activities

32. Zango's various bad acts have triggered massive user complaints. A Google search for "Zango" yields two different ads for spyware removers – companies that know that users searching for "Zango" are likely to need assistance removing spyware from their computers. Furthermore, a Google search for "zango spyware" yields more than 200,000 different results – many of them consumer complaints about Zango's practices.

33. Zango has also faced attention from regulators. After a lengthy investigation by the FTC, Zango entered into a settlement that required widespread changes to Zango's business practices – including ceasing nonconsensual installations onto users' computers, as well as paying a $3 million fine.[12] The FTC's complaint specifically alleged that Zango had deceptively failed to adequately disclose its software, that Zango had unfairly installed adware, and that Zango had unfairly failed to provide a reasonable means to remove its software.[13]

---

[12] http://www.ftc.gov/os/caselist/0523130/index.shtm
[13] http://www.ftc.gov/os/caselist/0523130/0523130cmp061103.pdf, page 4

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

Zango's Recent Activities

Zango Continues to Violate Its Settlement with the FTC

34. Zango claims to be in compliance with its recent settlement with the FTC. But in my testing, I have uncovered widespread violations of that settlement. My November 2006 "Bad Practices Continue at Zango, Notwithstanding Proposed FTC Settlement and Zango's Claims" details some of these violations.[14]

35. The FTC settlement requires Zango to label its ads.[15] But in fact Zango widely shows in-toolbar ads without any labeling whatsoever.[16] This is a simple, direct, and widespread violation of Zango's settlement obligations. As explained in paragraph 28, Zango also continues to show some unlabeled pop-up ads.

36. The FTC settlement further requires Zango to install its software only with "express consent," including "clear and prominent" disclosure of the material terms of Zango's software.[17] I have specifically documented counterexamples showing Zango software still violating these obligations.[18] I continue to find more such examples. For example, in testing of April 28, 2007, I downloaded a program that claimed to be a free media converter. After I scrolled past more than *sixty* on-screen pages of dense license agreement text, I finally learned that this media converter would install Zango software too. Such an obscure disclosure cannot satisfy the FTC's requirement of "clear and prominent" notice.

Zango Installers Still Fall Short of Informed Consent

37. Zango's recent installations continue to rely on misleading descriptions of Zango's software. In November 2006 testing, I found that Zango described its software as "display[ing] several ads per day."[19] This description fails to mention that Zango's ads appear in

---

[14] http://www.benedelman.org/news/112006-1.html
[15] http://www.ftc.gov/os/caselist/0523130/0523130agree061103.pdf, page 7
[16] http://www.benedelman.org/news/112006-1.html#h
[17] http://www.ftc.gov/os/caselist/0523130/0523130agree061103.pdf, pages 3 and 5
[18] http://www.benedelman.org/news/112006-1.html
[19] http://www.benedelman.org/spyware/images/zango-nov06/sexybabesx-111606.png

pop-ups, a format users are known to strongly dislike.[20] Alluding to the privacy effects of Zango's software, Zango describes its ads as "based upon keywords from your Internet browsing." But this disclosures glosses over Zango's true privacy consequences, as set out in paragraphs 18 to 20, i.e. tracking each user's specific searches and site visits. The omitted characteristics are material, in that reasonable users would want to consider these facts when evaluating Zango's offer. Yet Zango nonetheless omits these facts when asking users to install.

38. Zango attaches a declaration from Richard Purcell, who opines that "users who download Zango products are provided explicit notice about the program's capabilities and features."[21] But Purcell misunderstands Zango's obligations under the FTC settlement. The FTC settlement does not merely call for disclosure of the "capabilities and features" (i.e. benefits) of Zango's software. Rather, the FTC demands disclosure of *all material effects*[22] – crucially including *detriments*. It is in disclosing the software's detriments that Zango falls short – in many instances failing to prominently disclose that Zango's ads appear in much-hated pop-ups, and failing to disclose the privacy consequences of installing Zango software, even though these are material effects reasonable users would want to know about.

39. Zango also continues to use misleading installations predicated on misrepresentations of Zango's purpose. Zango widely solicits installation via ads promising to "stop junk emails" – a function wholly unrelated to Zango's display of pop-up ads. Furthermore, some Zango ads show a "fake user interface" design – falsely suggesting that the ads are messages from software already installed on a user's computer, when in fact the ads are merely solicitations unrelated to any program a user already runs.

40. Zango continues to solicit installations through advertisements shown through other vendors' spyware. For example, in November 2006 I observed Fullcontext spyware

---

[20] See e.g. http://www.itfacts.biz/index.php?id=P2176
[21] Purcell declaration at ¶8
[22] http://www.ftc.gov/os/caselist/0523130/0523130agree061103.pdf, page 3

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

injecting a banner ad for Zango into the top of the Google site.[23] Fullcontext spyware placed an ad above the logo, in a place where Google does not sell advertising to any company at any price. But using Fullcontext spyware, the Google home page showed an ad for Zango – without Google's permission.

41. Zango claims that on January 1, 2006, it ceased all nonconsensual installations.[24] But I personally observed Zango installing without consent on February 17, 2006. I even posted video proof of my observation,[25] and Zango itself conceded that nonconsensual installations occurred.[26] My personal first-hand observation directly contradicts Zango's puzzling claim that "Zango can be certain … that all users who have installed Zango's applications or products since January 1, 2006 have done so consensually"[27] – in that my video specifically shows a post-January-2006 Zango installation without user consent.

Zango Still Falls Short of Transparent Operation

42. Zango continues to operate in ways that are contrary to the reasonable expectations of typical users – including showing ads not attributed to Zango, and tracking and transmitting information unnecessarily and through hidden programs.

43. Zango continues to harm users' privacy and information security as set out in paragraphs 18 to 20, above.

44. Zango continues to show unlabeled in-toolbar ads, as set out in paragraph 35, above. I and others have recently observed further unlabeled Zango pop-up ads, as set out in paragraph 28.

45. The Zango toolbar tracks and transmits users' searches and site visits even when toolbar is disabled. Even if a user invokes Internet Explorer's View-Toolbars function to disable

---

[23] http://www.benedelman.org/news/112006-1.html#g
[24] TRO Motion, page 4
[25] http://www.benedelman.org/news/022006-1.html
[26] http://blog.180solutions.com/PermaLink,guid,b0fc12f9-e1f0-4a7a-998f-0b2f11d1fafd.aspx
[27] TRO Motion, page 4

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

Zango's toolbar, Zango's toolbar continues to transmit detailed information to its servers about users' browsing. These transmissions provide users with no benefit whatsoever, but they intrude on users' privacy

Zango Ads Continue to Defraud Internet Advertisers

46. Zango continues to defraud Internet advertisers by claiming commission improperly through their "cost per action" (CPA) advertising programs. For example, in "Spyware Still Cheating Merchants and Legitimate Affiliates," I showed Zango and its advertiser partners attempting to claim commission from Netflix when users specifically and directly requested the Netflix site.[28] Since users specifically requested, Netflix ought not have to pay commission for any resulting purchases. But Zango and its ads seek to receive commission from Netflix, as if the user's purchase was the result of Zango's promotional efforts.

47. I have also observed Zango ads performing click fraud through leading pay-per-click ad networks. For example, in "The Spyware - Click-Fraud Connection -- and Yahoo's Role Revisited," I showed Zango ads performing click fraud against Yahoo's pay-per-click ad network.[29] Yahoo's advertisers are only supposed to have to pay Yahoo a fee when users actually *click* on a pay-per-click ad. But because Zango and its advertiser partners perform click fraud, advertisers have to pay even if users don't click.

PC Tools' Current Detection of Zango Software

48. I have conducted tests to determine how PC Tools Starter Edition currently classifies Zango software and what action PC Tools Starter Edition takes upon finding Zango on a test PC.

49. To conduct these tests, I prepared a test PC (virtual machine) in my office. This PC had never before run either Zango or any PC Tools software. In testing of May 30, 2007, I installed Zango software, then downloaded the Google Pack which came with a copy of PC

[28] http://www.benedelman.org/news/052107-1.html
[29] http://www.benedelman.org/news/040406-1.html

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

Tools Starter Edition. I ran a default scan, and PC Tools ultimately detected Zango. The detection was labeled "Threat level: Info." PC Tools did not automatically remove Zango. After the PC Tools scan was complete, I tested the Zango software and confirmed that it was still operational.

50. Based on this test, I cannot agree with Zango's claim that "the version of Spyware Doctor that is on the Google website continues to damage and delete Zango products without user consent."[30] To the contrary, Spyware Doctor removes Zango only if users so instruct.

Characterizations of Zango's Software

51. In my view, the label "spyware" is an appropriate characterization of Zango's software. As set out in paragraphs 22 to 24, Zango software has been widely installed onto users' computers without user consent. As set out in paragraphs 18 to 20, Zango software transmits detailed information about users' browsing and searching. The combination of these two characteristics is correctly characterized as "spyware" – tracking users' activities, and doing so without users' consent.

52. The label "spyware" remains appropriate even though Zango has recently ceased nonconsensual installations. For one, the label is appropriate as to prior installations, some of which may still be present on some users' computers. Second, as set out in paragraph 37, Zango's current installations are misleading and fail to convey key details users need to know in order to evaluate Zango's offer. Finally, the term "spyware" has become a generic catch-all for software installed on users' computers, taking action to users' detriment (e.g. by tracking browsing or showing ads), no matter how such software is installed.[31]

53. In my view, the label "malicious" is an appropriate characterization of all of Zango's software. As set out in paragraphs 46 and 47, Zango's software defrauds Internet

---

[30] TRO Motion, page 7

[31] See e.g. the much-cited definition of "spyware (and other potentially unwanted technologies" offered by the Anti-Spyware Coalition. http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm

advertisers by claiming commissions and payments to which Zango and its advertisers have no valid right. Such improper claims are the essence of fraud, and these actions are malicious even when advertisers fail to take action to protect themselves. Secondarily, as set out in paragraph 37, Zango has systematically failed to describe its software using the key terms (e.g. "pop-up ads") necessary for users to fully and quickly understand the effects of installing Zango. This mischaracterization occurs to Zango's benefit but to users' detriment – entirely consistent with the conclusion that Zango's actions are malicious.

54. In my view, the label "infection" is an appropriate characterization of Zango's software. The term "infection" is generally used in the computer security industry to describe programs that enter users' computers without users' informed consent, and that have effects reasonable users would not approve.[32] These characteristics match Zango's behavior. Furthermore, other security software widely uses the term "infection" to describe detected programs – even programs that lack Zango's history of nonconsensual installations.[33]

Similarities and Differences between Seekmo and Other Zango Software

55. Zango's Seekmo product is substantially the same as Zango's other software – identical in its display of pop-up ads and in its tracking of user activities. But while I have seen Zango installed without consent, I have never seen such installation of Seekmo. And although I have widely seen Zango promoted through other vendors' spyware, such promotion is less widespread as to Seekmo. Thus, Seekmo users are somewhat more likely than other Zango users to have received a meaningful opportunity to evaluate the Seekmo software and grant or deny consent for it to install.

56. In my testing, Zango's four current programs (Zango, Seekmo, Hotbar, and Spam Blocker) all share a variety of components. That is, a user who installs Zango and a user who

---

[32] See e.g. http://www.webroot.com/resources/spywareinfo/infection.html, http://antivirus.about.com/od/securitytips/a/removespyware.htm, http://www.eweek.com/article2/0,1759,1771220,00.asp

[33] See e.g. http://www.webroot.com/company/pressroom/pr/state-of-spyware-Q206.html

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

installs Seekmo each receive certain files and registry entries that are common to both installations. Because these components come with both programs, there is no clear way to know whether a given component arrived through Zango or instead through Seekmo, Hotbar, or Spam Blocker. As a result, it is difficult for a security vendor or outside analyst to classify these components as belonging to one specific Zango program rather than to several or all of them.

57. The inevitable result of Zango's decision to share components across programs is that security software detects some components as one Zango program, and other components as another. To the extent that security software treats different Zango programs differently, e.g. as a result of different prior practices previously observed, the associated components will also be treated differently. To correct this problem, Zango need only make each components unique to a particular single program.

Implications of This Case for Consumers and The Computer Security Industry

58. Spyware is a substantial harm to typical consumer users. The National Cyber Security Alliance estimates that 61% of home computers are infected with at least one spyware program.[34] If repair costs even a few dollars of users' time (not to mention the cost of specialized hardware or professional assistance), the resulting cost to the economy reaches hundreds of millions of dollars.

59. Typical users have great difficulty removing spyware from their computers. Anti-spyware software provides crucial assistance to keeping users' computers operational and reliable. Anti-spyware software therefore serves an important public function. Just as courts are rightly deferential to the editorial recommendations of *Consumer Reports*, courts should hesitate to interfere with the operations of anti-spyware software.

60. Zango is part of the spyware problem. Webroot's December 2006 report found Zango to be the most prevalent of all "adware"-type spyware threats.[35] Sunbelt's current "Real

---

[34] http://www.staysafeonline.info/pdf/safety_study_2005.pdf
[35] http://www.webroot.com/resources/spywareinfo/topthreats-december06.html

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

time Spyware Threats" listing lists Zango's Hotbar and Zango Toolbar among the "top 10 spyware threats … for the past week."[36] Zango's use of thousands of distributors, without rigorous oversight or control, pumped millions of dollars into the spyware ecosystem – damaging tens of millions of computers in the process.

61. Zango's repeated promises of reform demonstrate why security providers should consider a software vendor's history when evaluating the vendor's promises and claims of reform. Zango seems to take the position that, having purportedly addressed at least the most egregious of its prior bad acts, it now can no longer be classified with an eye towards its prior behavior. But some of Zango's tens of millions of old installations – including prior nonconsensual installations – still remain to be cleaned off of users' computers. More generally, Zango's accumulated reputation is an appropriate factor to consider when evaluating whether reasonable users would want Zango on their computers. Reputation is particularly important when evaluating whether Zango can be trusted to comply with its privacy policy and to otherwise act as a trustworthy steward of the information it receives. Zango's sordid past provides ample basis to doubt the company's behavior going forward. Any reasonable security expert would consider this information in reaching a conclusion as to the desirability of Zango's software. In my view, PC Tools ought to be free to consider this information too.

I declare under penalty of perjury that the foregoing is true and correct and that this declaration was executed on May 31, 2007, at Cambridge, Massachusetts.

Benjamin G. Edelman, Ph.D., J.D., M.A.

[36] http://research.sunbelt-software.com/Default.aspx

STOEL RIVES LLP
ATTORNEYS
600 University Street, Suite 3600, Seattle, WA 98101
Telephone (206) 624-0900

CERTIFICATE OF SERVICE

I hereby certify that on May 31, 2007, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following persons:

- **Michael Rosenberger**
  mrosenberger@gordontilden.com,chudson@gordontilden.com, jbukowski@gordontilden.com
- **Jeffrey I Tilden**
  jtilden@gordontilden.com,eevans@gordontilden.com, jbukowski@gordontilden.com
- **Conor F Farley**
  cfarley@hollandhart.com
- **Tarek F M Saad**
  tfsaad@hollandhart.com

DATED: May 31, 2007 at Seattle, Washington.

/s/ ______________________________
J. Ronald Sim, WSBA No. 4888
Maren R. Norton, WSBA No. 35435
STOEL RIVES L.L.P.
600 University Street, Suite 3600
Seattle, WA 98101-3197
Telephone: 206-624-0900
Fax: 206-386-7500
jrsim@stoel.com
mnorton@stoel.com

ATTORNEYS FOR DEFENDANT

27a Linnaean St.
Cambridge, MA 02138

Benjamin G. Edelman

ben@benedelman.org
(617) 379-0820

Experience

Assistant professor, Harvard Business School. Negotiations, Organizations & Markets unit. (April 2007 – present)
Fields: Industrial organization, market design, information economics.
Research interests: Electronic markets. Internet advertising, reputation, and fraud. Automated data collection.
Anticipated teaching: Market design, negotiation.

Independent consultant and expert witness (November 1999 – present)
Conducted quantitative analyses and empirical testing for a variety of clients including the American Civil Liberties Union, National Association of Broadcasters, National Football League, New York Times, and Washington Post on topics including online advertising, marketing fraud, spyware, spam, pay-per-click advertising and click fraud, Internet filtering, geolocation and targeting, privacy, security, automated data collection, and user interface design. Qualified as an expert in Federal court on multiple occasions, and provided oral testimony under direct and cross examination.

Student Fellow / Technology Analyst, Berkman Center for Internet & Society (May 1998 – January 2004)
Conducted empirical studies of the Internet's domain name system, peer-to-peer filesharing, spyware/adware, content filtering by network intermediaries. Developed software systems for interactive real-time communication among class/meeting participants. Designed and operated system for webcast of and remote participation in numerous Berkman Center, Harvard Law School, and Cambridge community events as well as twelve ICANN public meetings.

Education

Harvard Graduate School of Arts & Sciences - Ph.D., Economics, 2007.
Dissertation: "Topics in Internet Advertising"
Advisors: Ariel Pakes, Alvin Roth, David Parkes.

Harvard Law School - J.D., 2005.

Harvard Graduate School of Arts & Sciences - A.M., Statistics, 2002.

Harvard College - A.B., Economics, *summa cum laude*, 2002; Phi Beta Kappa.

Woodrow Wilson Senior High School - Washington, DC: 1998; valedictorian.

Representative Research

Internet Advertising and the Generalized Second Price Auction (*American Economic Review*, March 2007)
with Michael Ostrovsky and Michael Schwarz

Strategic Bidder Behavior in Sponsored Search Auctions (*Decision Support Systems*, February 2007) with Michael Ostrovsky

Adverse Selection in Online "Trust" Certifications (2006) www.benedelman.org/publications/advsel-trust-draft.pdf

Optimal Contracting when Judgment-Proof Agents Are Paid in Arrears (forthcoming)

Assessing and Improving the Safety of Internet Search Engines (2006) (published in *The Rising Power of Search Engines on the Internet*)

Earnings and Ratings at Google Answers (2004) cyber.law.harvard.edu/people/edelman/pubs/googleanswers-011404.pdf

Web Sites Sharing IP Addresses: Prevalence and Significance (2003) cyber.law.harvard.edu/people/edelman/ip-sharing

Empirical Analysis of Internet Filtering in China (2002) with Jonathan Zittrain cyber.law.harvard.edu/filtering/china
Published in *IEEE Internet Computing* as "Internet Filtering in China" (March-April 2003)

The Effect of Editorial Discretion Book Promotion on Sales at Amazon.com (2001-2002) benedelman.org/pubs/thesis-intro.pdf
Seymour and Ruth Harris Prize for Best Thesis in Economics, Thomas Temple Hoopes Prize for Undergraduate Research

EXHIBIT
A

18 of 22

Long-Term Research Projects

"Spyware": Research, Testing, Legislation, and Suits (2002-2007) benedelman.org/spyware

Strategies and Outcomes in Search Engines' Pay-Per-Click Listings (2004-2007) with Michael Ostrovsky and Michael Schwarz

Resources for Affiliates and Affiliate Merchants (2004-2007) benedelman.org/affiliates

Documentation of Internet Filtering Worldwide (2002-2003) with Jonathan Zittrain cyber.law.harvard.edu/filtering

Localized Google Search Result Exclusions (2002-2003) with Jonathan Zittrain cyber.law.harvard.edu/filtering/google

The Top-Level Domain Evaluation Project (2002-2003) with Jonathan Zittrain cyber.law.harvard.edu/tlds

Classroom and Meeting Technology Tools (1998-2002) cyber.law.harvard.edu/meetingtools

Software Environments for Online Deliberative Discourse (1999-2000) cyber.law.harvard.edu/projects/deliberation

ICANN Public Meeting Archives, Notes, and Briefing Books (1998-2001) cyber.law.harvard.edu/icann cyber.law.harvard.edu/ifwp

Additional Writings

Spyware Still Cheating Merchants and Legitimate Affiliates (2007) benedelman.org/news/052107-1.html

How Spyware-Driven Forced Visits Inflate Web Site Traffic Counts (2007) benedelman.org/news/050707-1.html

Advertising Through Spyware -- After Promising To Stop (2007) benedelman.org/news/031407-1.html

Why I Can Never Agree with Adware and Spyware (2007) technology.guardian.co.uk/online/insideit/story/0,,1997629,00.html

Bad Practices Continue at Zango, Notwithstanding Proposed FTC Settlement and Zango's Claims (2006) with Eric Howes benedelman.org/news/112006-1.html

Intermix Revisited (2006) benedelman.org/news/110806-1.html

Current Ask Toolbar Practices (2006) benedelman.org/spyware/ask-toolbars

False and Deceptive Pay-Per-Click Ads (2006) benedelman.org/ppc-scams

Cookies Detected by Anti-Spyware Programs: The Current Status (2006) www.vinnylingham.com/specialreports/cookiedetections

How Vonage Funds Spyware (2006) benedelman.org/news/071806-1.html

Spyware Showing Unrequested Sexually-Explicit Images (2006) benedelman.org/news/062206-1.html

Banner Farms in the Crosshairs (2006) benedelman.org/news/061206-1.html

The Safety of Internet Search Engines (2006) siteadvisor.com/studies/search_safety_may2006 with Hannah Rosenbaum

New York v. Direct Revenue, LLC - Documents and Analysis (2006) benedelman.org/spyware/nyag-dr

The Spyware - Click-Fraud Connection - and Yahoo's Role Revisited (2006) benedelman.org/news/040406-1.html

Advertisers Funding Direct Revenue (2006) benedelman.org/spyware/images/dr-mar06

Critiquing ITSA's Pro-Adware Policy (2006) benedelman.org/news/033106-2.html

Advertisers Funding 180solutions (2006) benedelman.org/spyware/images/180-jan06

Nonconsensual 180 Installations Continue (2006) benedelman.org/news/022006-1.html

Pushing Spyware through Search (2006) benedelman.org/news/012606-1.html

Affiliate Hall of Shame (2006) benedelman.org/news/011606-1.html

180solutions's Misleading Installation Methods - Dollidol.com (2006) benedelman.org/spyware/installations/dollidol-180

Scanning for Solutions (2005) publications.mediapost.com/index.cfm?fuseaction=Articles.san&s=37284

What Claria Doesn't Disclose (Any More) (2005) benedelman.org/news/111505-1.html

Claria Shows Ads Through Exploit-Delivered Popups (2005) benedelman.org/news/101805-1.html

Video: New.net Installed through Security Holes (2005) benedelman.org/news/100505-1.html

How Affiliate Programs Fund Spyware (2005) benedelman.org/news/091405-1.html

How Expedia Funds Spyware (2005) benedelman.org/news/090705-1.html

How Yahoo Funds Spyware (2005) benedelman.org/news/083105-1.html

What Passes for "Consent" at 180solutions (2005) benedelman.org/news/062805-1.html

Google's Role: Syndicated Ads Shown Through Ill-Gotten Third-Party Toolbars (2005) benedelman.org/news/060605-1.html

Ask Jeeves Toolbar Installs via Banner Ads at Kids Sites (2005) benedelman.org/spyware/installations/askjeeves-banner

Hotbar Installs via Banner Ads at Kids Sites (2005) benedelman.org/spyware/installations/kidzpage-hotbar

The 180 Turnaround That Wasn't (2005) adbumb.com/adbumb159.html

The PacerD Installation Bundle (2005) benedelman.org/spyware/installations/pacerd

Claria's Misleading Installation Methods - Ezone.com (2005) benedelman.org/spyware/installations/ezone-claria

Claria's Misleading Installation Methods - Dope Wars (2005) benedelman.org/spyware/installations/dopewars-claria

180solutions's Misleading Installation Methods - Ezone.com (2005) benedelman.org/spyware/installations/ezone-180

3D Desktop's Misleading Installation Methods (2005) benedelman.org/spyware/installations/3d-screensaver

Comparison of Unwanted Software Installed by P2P Programs (2005) benedelman.org/spyware/p2p

Advertisers Supporting eXact Advertising (2005) benedelman.org/spyware/exact-advertisers

How Google's Blogspot Helps Spread Unwanted Software (2005) benedelman.org/news/022205-1.html

How VeriSign Could Stop Drive-By Downloads (2005) benedelman.org/news/020305-1.html

Intermediaries' Role in the Spyware Mess (2005) benedelman.org/news/052305-1.html

Media Files that Spread Spyware (2005) benedelman.org/news/010205-1.html

Video: Ebates Installed through Security Holes (2004) benedelman.org/news/121504-1.html

Direct Revenue Deletes Competitors from Users' Disks (2004) benedelman.org/news/120704-1.html

Who Profits from Security Holes? (2004) benedelman.org/news/111804-1.html

Gator's EULA Gone Bad (2004) benedelman.org/news/112904-1.html

Grokster and Claria Take Licenses to New Lows, and Congress Lets Them Do It (2004) benedelman.org/news/100904-1.html

California's Toothless Spyware Law (2004) benedelman.org/news/092904-1.html

The Effect of 180solutions on Affiliate Commissions and Merchants (2004) benedelman.org/spyware/180-affiliates

WhenU Spams Google, Breaks Google "No Cloaking" Rules (2004) benedelman.org/spyware/whenu-spam

WhenU Copies 26+ Articles from 20+ News Sites (2004) benedelman.org/spyware/whenu-copy

Advertisers Using WhenU (2004) benedelman.org/spyware/whenu-advertisers

WhenU Security Hole Allows Execution of Arbitrary Software (2004) benedelman.org/spyware/whenu-security

WhenU Violates Own Privacy Policy (2004) benedelman.org/spyware/whenu-privacy

Methods and Effects of Spyware (FTC Comments) (2004) benedelman.org/spyware/ftc-031904.pdf

A Close Reading of Utah's Spyware Control Act (2004) benedelman.org/spyware/utah-mar04

Web Sites Sharing IP Addresses: Prevalence and Significance (2003) cyber.law.harvard.edu/people/edelman/ip-sharing

Documentation of Gator Advertisements and Targeting (2003) cyber.law.harvard.edu/people/edelman/ads/gator

Empirical Analysis of Google SafeSearch (2003) cyber.law.harvard.edu/people/edelman/google-safesearch

Large-Scale Registration of Domains with Typographical Errors (2003) cyber.law.harvard.edu/people/edelman/typo-domains

Technical Responses to Unilateral Internet Authority: The Deployment of VeriSign "Site Finder" and ISP Response (2003) with Jonathan Zittrain cyber.law.harvard.edu/tlds/sitefinder

Compliance with UDRP Decisions: A Case Study of Joker.com (2003) cyber.law.harvard.edu/people/edelman/udrp-compliance

Blocked Sites will Return, but with Limited Access (2003) South China Morning Post, op-ed

Domain Name Typosquatter Still Generating Millions (2003) circleid.com/article/101_0_1_0_C

Documentation of Internet Filtering in Saudi Arabia (2002) with Jonathan Zittrain cyber.law.harvard.edu/filtering/saudiarabia

Localized Google Search Result Exclusions (2002) wth Jonathan Zittrain cyber.law.harvard.edu/filtering/filtering/google

Analysis of Domain Reregistrations Used for Distribution of Sexually-Explicit Content (2002)
cyber.law.harvard.edu/people/edelman/renewals

Large-Scale Intentional Invalid WHOIS Data: A Case Study of "NicGod Productions" / "Domains For Sale" (2002)
cyber.law.harvard.edu/people/edelman/invalid-whois

.NAME Registrations Not Conforming to .NAME Registration Restrictions (2002)
cyber.law.harvard.edu/people/edelman/name-restrictions

Alternative Perspectives on Registrar Market Share (2002) cyber.law.harvard.edu/people/edelman/registrar-choice

DNS as a Search Engine: A Quantitative Evaluation (2002) cyber.law.harvard.edu/people/edelman/dns-as-search

Disputed Registrations in .BIZ (2002) cyber.law.harvard.edu/people/edelman/biz-sunrise

TLD Registration Enforcement: A Call for Automation (2002) circleid.com/article/66_0_1_0_C circleid.com/article/72_0_1_0_C

Invalid WHOIS Data: Who Is Responsible? (2002) circleid.com/article/79_0_1_0_C

When the Net Goes Dark and Silent (2002) South China Morning Post, op-ed

Defensive Registrations: Why They're Still Needed, and How to Make Them Earn Their Keep (2002)
Verisign Digital Brand Management Digital Branding Bulletin, www.verisign.com/services/cdns/news/columnist_200212.html

iCravetv.biz/Entervision Retransmits CNN, Cartoon Network, PAX TV, California NBC Affiliate (2002)
cyber.law.harvard.edu/people/edelman/icrave

Analysis of Registrations in Alternative Root TLDs (2001) cyber.law.harvard.edu/people/edelman/dotbiz and /people/edelman/dotweb

Documentation of Privacy and Security Shortcomings at Buy.com (2000) cyber.law.harvard.edu/people/edelman/buy-privacy.html

Understanding and Critiquing ICANN's Policy Agenda (2000) cyber.law.harvard.edu/icann/pressingissues2000/briefingbook

Executive Summaries of Formative ICANN Documents (1999)
cyber.law.harvard.edu/pressbriefings/icann/briefingbook/executivesummaries.html

ICANN and the Public Interest: Pressing Issues (1999) cyber.law.harvard.edu/icann/workshops/la/briefingbook

Using Trumpet Winsock on Netcom Netcruiser Accounts (1995) cyber.law.harvard.edu/people/edelman/trumpet.html

Programming Experience

Microsoft Visual Basic (14+ years experience), VB.NET, VBA, VBS, ASP, ADO, OLEDB

Mathworks MatLab	Stata	SPlus / R
Python	PHP	

Recent Awards

Harvard University Graduate Economics Fellowship (2003-2006)

John M. Olin Fellowship in Law and Economics (2003-2004, 2004-2005)

Hoopes Prize for Undergraduate Research (2002)

Seymour and Ruth Harris Prize for Best Honors Thesis in Economics (2002)

John Harvard Scholarship, Harvard College (1998-1999, 1999-2000, 2000-2001)

Rank I Honors, Harvard College (1998-1999, 1999-2000, 2000-2001)

Phi Beta Kappa, Harvard College (2001)

Undergraduate Honors Research Scholarship, Department of Economics, Harvard College (2001)

Detur Prize, Harvard College (1999)

Expert Testimony

District Court, Third Judicial District of Utah (2004)

US Federal Court, Eastern District of Michigan (2003)

US House of Representatives, Committee on the Judiciary (2003)

US Federal Court, Eastern District of Pennsylvania (2002)

US Federal Court, Western District of Pennsylvania (2000)

Academic Service

Referee: *American Economic Review*, *Journal of Applied Economics*, Sponsored Search Workshop, Workshop on the Economics of Information Security, Workshop on the Economics of Securing the Information Infrastructure

Program Committee: Workshop on the Economics of Securing the Information Infrastructure (2006), Sponsored Search Workshop (2007)

Non-resident tutor, Cabot House – academic and thesis advising (2004-2007)